Safety of Unmanned Systems:

Joint Government/Industry Unmanned Systems Safety Workshop

Sponsored by DSOC ATP TF

Status Update

29 June 2006

Agenda

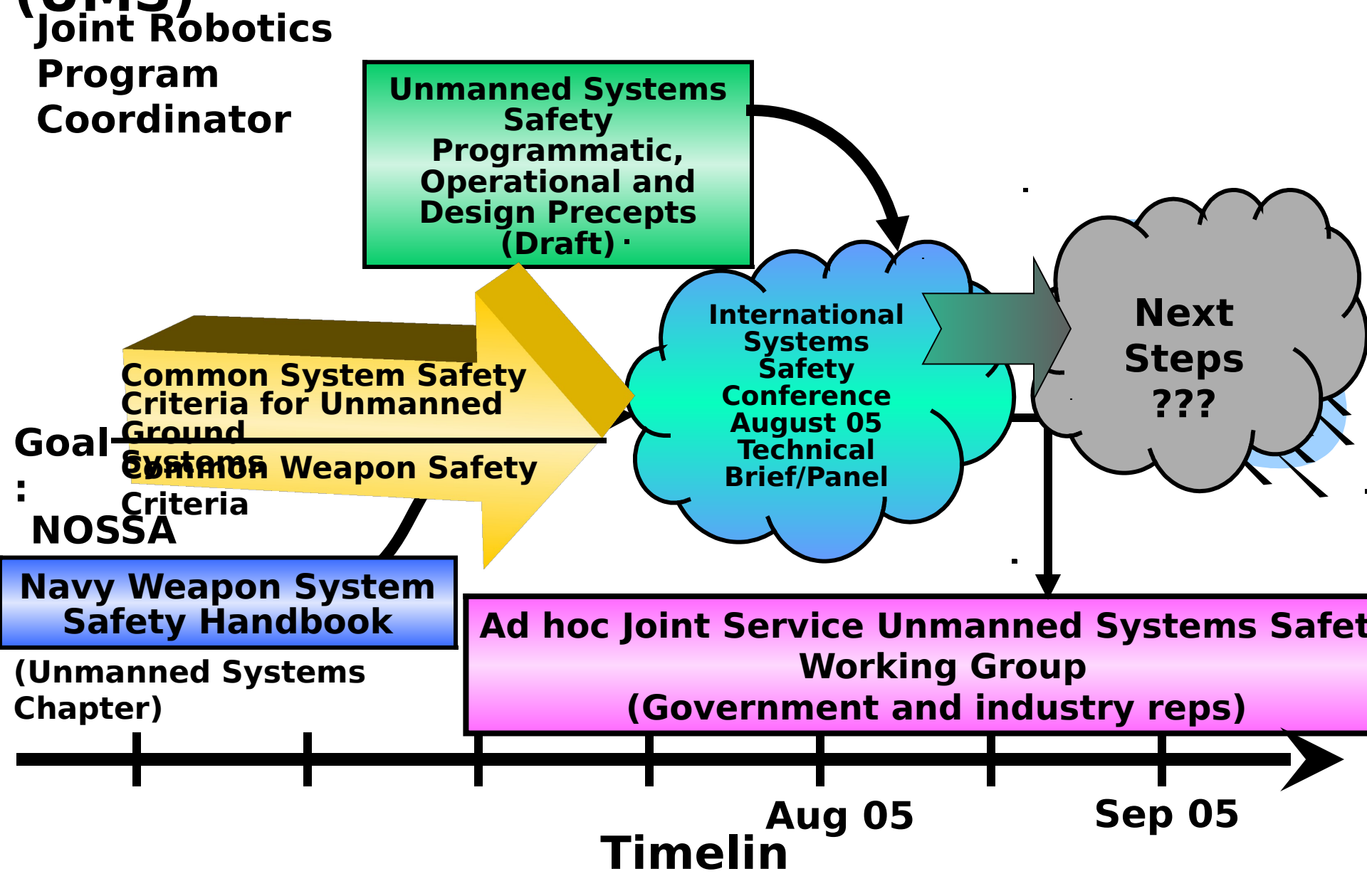
- Background
- Scope
- Task Objective
- Approach
- Schedule
- Progress
- Products
- Summary

Background

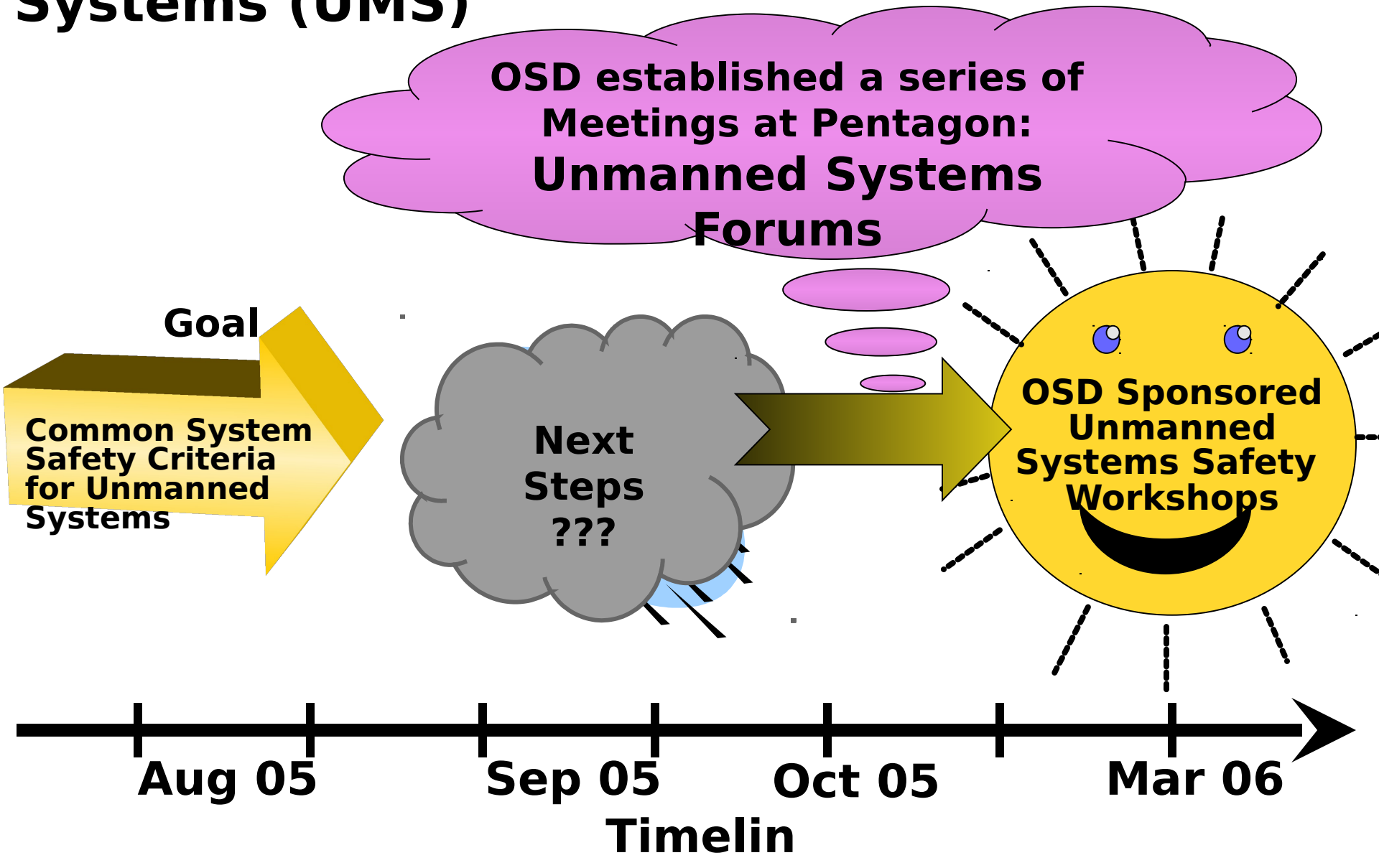
- Unmanned systems provide new capabilities to meet needs/mission requirements
- Numerous unmanned systems (UMS) are under development in each of the Military Services and other government agencies
- But, unmanned systems have unique challenges, e.g.
  - Integrated operations
  - System control and security
  - Target identification/verification
- No unified system safety approach

Unintended casualties could drastically impact design, development and use

Chronology for Safety of Unmanned Systems (UMS)

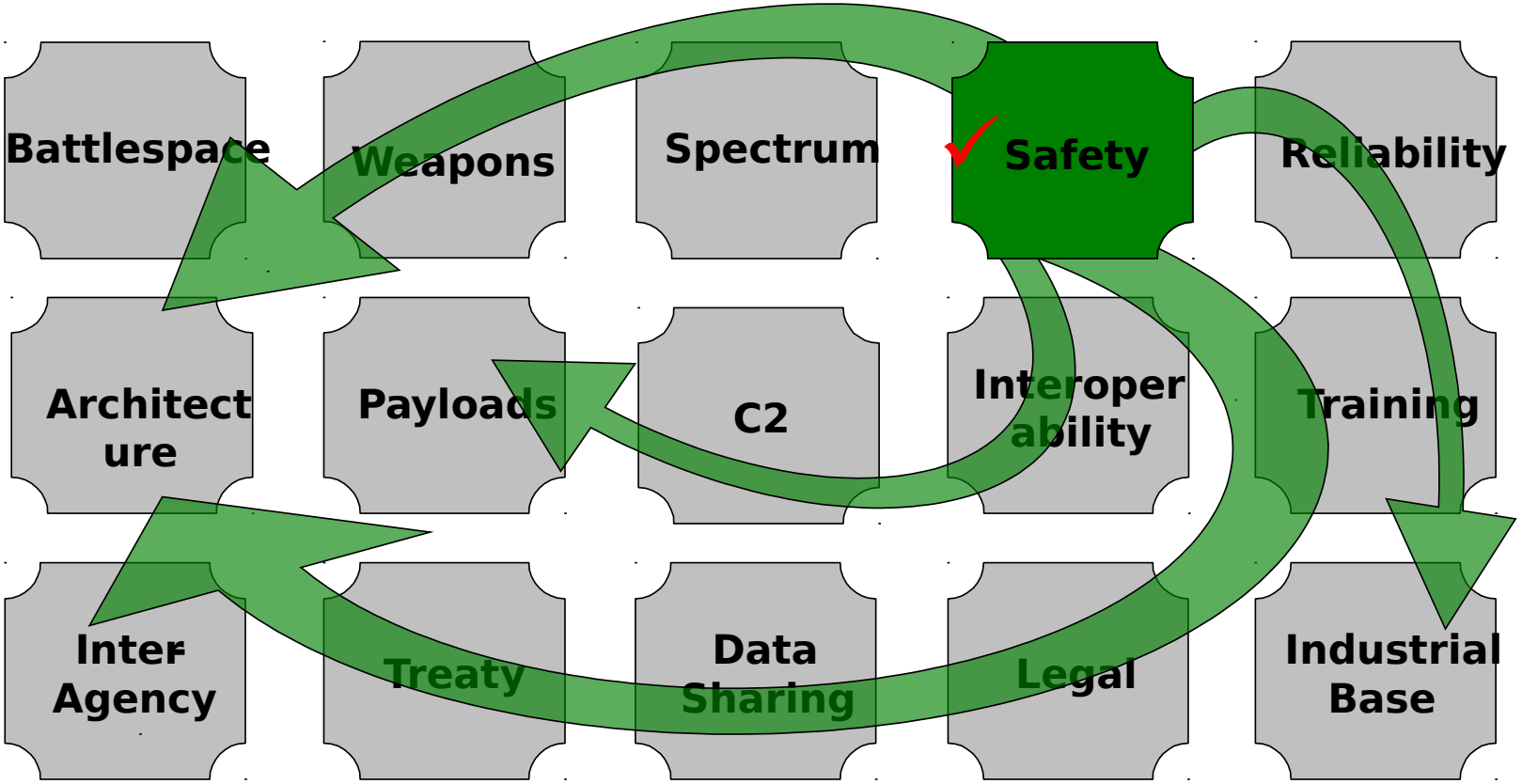

Joint Robotics Program Coordinator
Unmanned Systems Safety Programmatic, Operational and Design Precepts (Draft)
Common System Safety Criteria for Unmanned Ground Systems
Common Weapon Safety Criteria
International Systems Safety Conference August 05 Technical Brief/Panel
Next Steps ???
Goal:
NOSSA
Navy Weapon System Safety Handbook
(Unmanned Systems Chapter)
Ad hoc Joint Service Unmanned Systems Safet
Working Group
(Government and industry reps)
Aug 05
Sep 05
Timelin

Chronology for Safety of Unmanned Systems (UMS)



Scope:

Unmanned Systems Challenges



Slide from Mr. M. Schaeffer's brief of 28 March 06 at Unmanned Systems Safety Workshop, Huntsv

UMS Safety Objectives

- Focus the technical community on the System Safety needs for UMS
- Specifically
  - Understand the safety concerns, including legal issues, associated with the rapid development and use of a diverse family of unmanned systems both within, and external to, the DoD.
  - Establish and agree upon a standardized set of safety precepts to address the safety concerns associated with the design, operation, and programmatic oversight of all unmanned systems.
  - Develop safety guidance, such as design features, hazard controls and mitigators, for the design, development, and acquisition of unmanned systems.

Approach

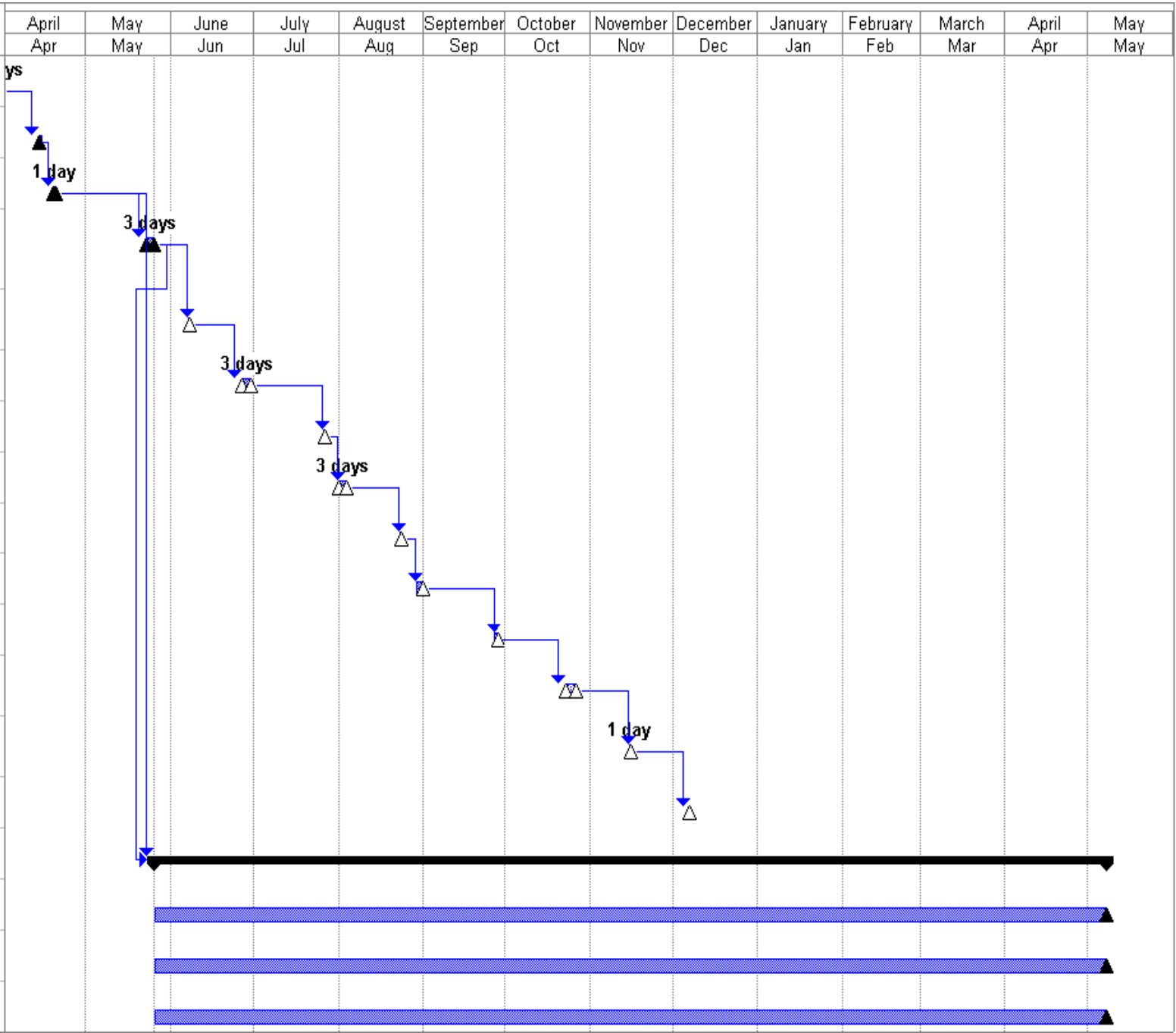
- **Involve technical community**
  - **Six Teams**
  - **Approximately 60 technical experts**
  - **Government, Industry, Academia**
- **Maximize Community Awareness**
  - **March Workshop**
    - **300 attendees**
  - **International Systems Safety Conference (ISSC)**
  - **AUVSI**
  - **NDIA Systems Engineering Conference**
- **Obtain Feedback**
  - **Web Page (http://www.ih.navy.mil/unmannedsystems)**
  - **Tech Panels**
    - **ISSC (31 July - 4 Aug 2006)**
    - **AUVSI (29 – 31 Aug 2006)**
    - **NDIA Systems Engineering (23 – 26 Oct 2006)**

March Workshop Accomplishments

- **Generated DRAFT OSD-wide UMS Safety Guidance**
- **Established process to refine OSD-wide UM Systems Safety guidance**
- **Developed POA&M for issuance of OSD Systems Safety guidance**
- **Enhanced communications at all levels**
  - Service PMs
  - Service technical and safety communities
  - Service safety boards
  - Between Services and industry reps
  - Established web page
    - **(http://www.ih.navy.mil/unmannedsystems)**

POA&M for DSOC ATP TF Unmanned Systems Safety Initiative

ID	Task Name
1	Unmanned Systems Workshop @ Huntsville, AL (Session I)
2	Post products on the web site & solicit comments
3	Status brief to OSD, Mr. Schaeffer, 19 April 06
4	Workgroups meet @ Crystal City forSesson II- refine products, post on web-site, & solict comments
5	Present Status of Unmanned Systems Workshop to DSOC ATP TF
6	Workgroups meet @ Crystal City for Session III - refine products
7	Status brief to OSD, Mr. Schaeffer, 20 July 06 (notional date)
8	Report out interim products @ ISSSC in Albuquerque (Panel Discussion)
9	Status brief to OSD, Mr. Schaeffer, 23 August 06
10	Report out interim products at AUVSI, Orlando (Panel Discussion)
11	Status brief to OSD, Mr. Schaeffer, 27 Sept 06 (notional date)
12	Report out interim products at NDIA Systems Engineering Conference, San Diego (Panel Discussion)
13	Final rpt to Mr. Schaeffer w/interim safety guidance & recommendations for publication
14	Issue Interim Guidance
15	**Continuing Long Term Actions**
16	Lessons Learned
17	Common Processes
18	Shared databases



Progress

- **Held Three Workshops**
  - **March 2006, Huntsville**
  - **May 2006, Crystal City**
  - **June 2006, Crystal City**
- **Developed Draft Safety Precepts**
  - **Programmatic safety precepts**
  - **Operational safety precepts**
  - **Design safety precepts**
- **Developing design safety “best practices”**
  - **Weapons control**
  - **Situational Awareness**

UMS Safety Precept Definitions

Progam Safety Precept (PSP) = Program Management Principles & Guidance that will help insure safety is adequately addressed throughout the lifecycle process.

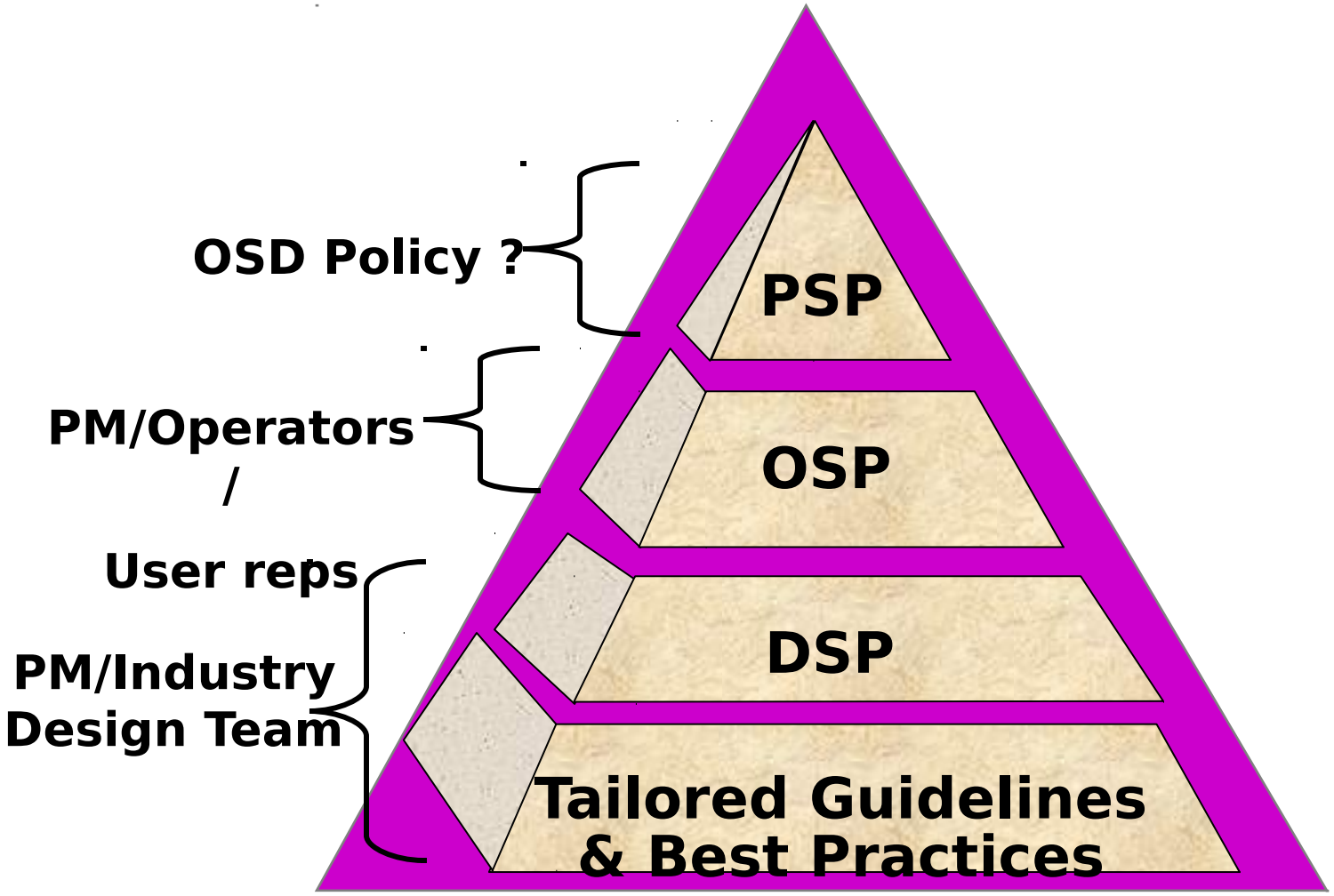
Operational Safety Precept (OSP) = Operational Guidelines that should be adhered to during system operation. They guide system design for operation use and provide the basis for design safety precept and more detail system safety design requirements.

Design Safety Precepts (DSP) = General Design Guidance intended to facilitate safety of the system and minimize hazards. Safety design precepts are intended to influence, but not dictate, specific design solutions.

Workshop Organization

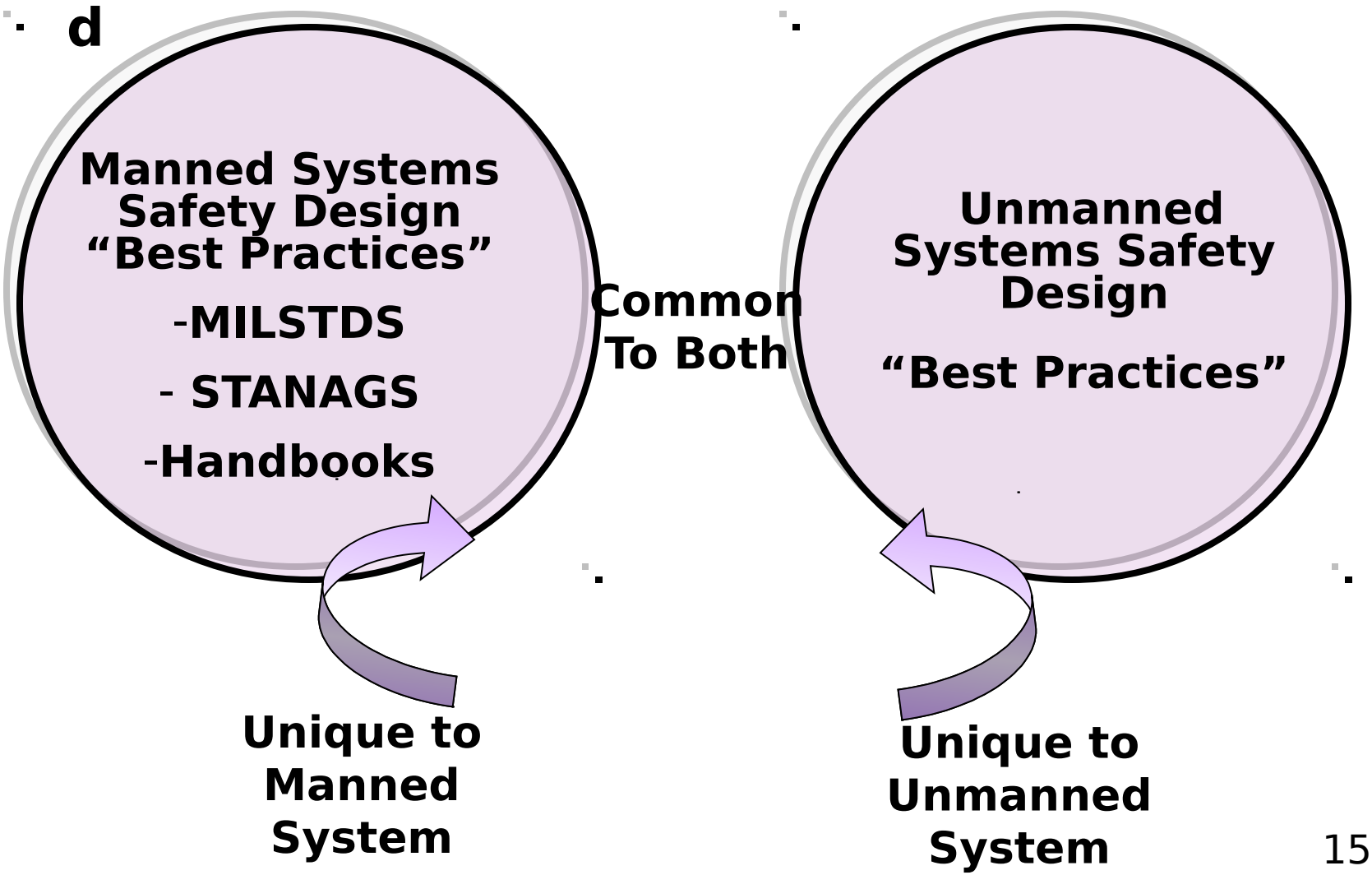
- **Six Workgroups**
  1. **Precepts**
  2. **Weapons Control**
  3. **Situational Awareness**
     - **Human-Machine Interface**
     - **Machine-Machine Interface**
  4. **Command and Control**
  5. **States and Modes**
  6. **Definitions/Common Taxonomy**

Safety Precepts for UMS



Provide program managers with appropriate safety guide and best practices, while maintaining PM's design flexibi

Safety Design Guidelines



Discussion of Products

Workgroup Moderators

- **Precepts: Mr. Josh McNeil (Army)**
  - Process for developing precepts
  - Discussion of selected precepts, as examples, including rationale for the precept
- **Weapons Control: Mr. Bill Pottratz (Army)**
- **Situational Awareness: Dr. Tom English (Navy)**
- **C^2: Mr. Steve Mattern (Apogen Technologies)**
- **States and Modes: Mr. Bob Schmedake (Boeing)**
- **Definitions: Mr. Danny Brunson (EG&G Inc)**

Precepts Work Group 1 Status

Josh McNeil
Army/SED

Weapons Control Work Group 2 Status

Bill Pottratz
AMCOM Safety

Group 2: Weapon Control

Participants

Air Force	**Preston Parker**
	Mark Handrop
	John Deep
Army	**Chris Janow**
	Mike Zecca
	Dave Magidson
	Chris Olson
Navy	**Jack Waller**
	Mary Ellen Caro
	John Filo
Industry	**Bill Blake**

Group 2: Weapon Control

- Purpose
  - Develop safety guidelines, that can be endorsed by various boards, for certification of unmanned system platforms and weapon interfaces
- Issues Addressed
  - Precepts
  - Safety Certification
  - Design Guidelines

Assumptions

- Workgroup recognizes the sufficiency of existing STANAG and MIL-STD’s for weapon systems.
- Functional contribution of other UMS subsystems to weapon safety system constitutes a distributed safety system. These contributing UMS subcomponents may be safety critical and must be designed, developed and maintained appropriately.
- Top level guidelines apply to all types of weapons – missiles, bombs, guns, directed energy devices, non-lethal systems

Precept 22

- The UMS platform shall be designed to incorporate a minimum of 2 independent safety features, each of which will prevent subsequent commanded (or uncommanded) launch/release/firing/arm enable of the weapon.
- The removal of each safety feature shall require a unique verified message generated as a consequence of a distinct authorized entity action (e.g. messages shall not originate within the UMS platform).
- The messages shall be sent in the proper sequence and acted upon only after being recognized as being in the proper sequence.

Associated Guidelines

- UMS subsystems shall not subvert or compromise the independence of weapon safety features.
- Each weapon/platform shall have unique identifier and shall respond only to commands with its identifier in the command.
- The UMS platform shall be designed to monitor and validate content and sequence of messages, and the response of the system to the messages, and take appropriate safing and notification actions.

Precept 29

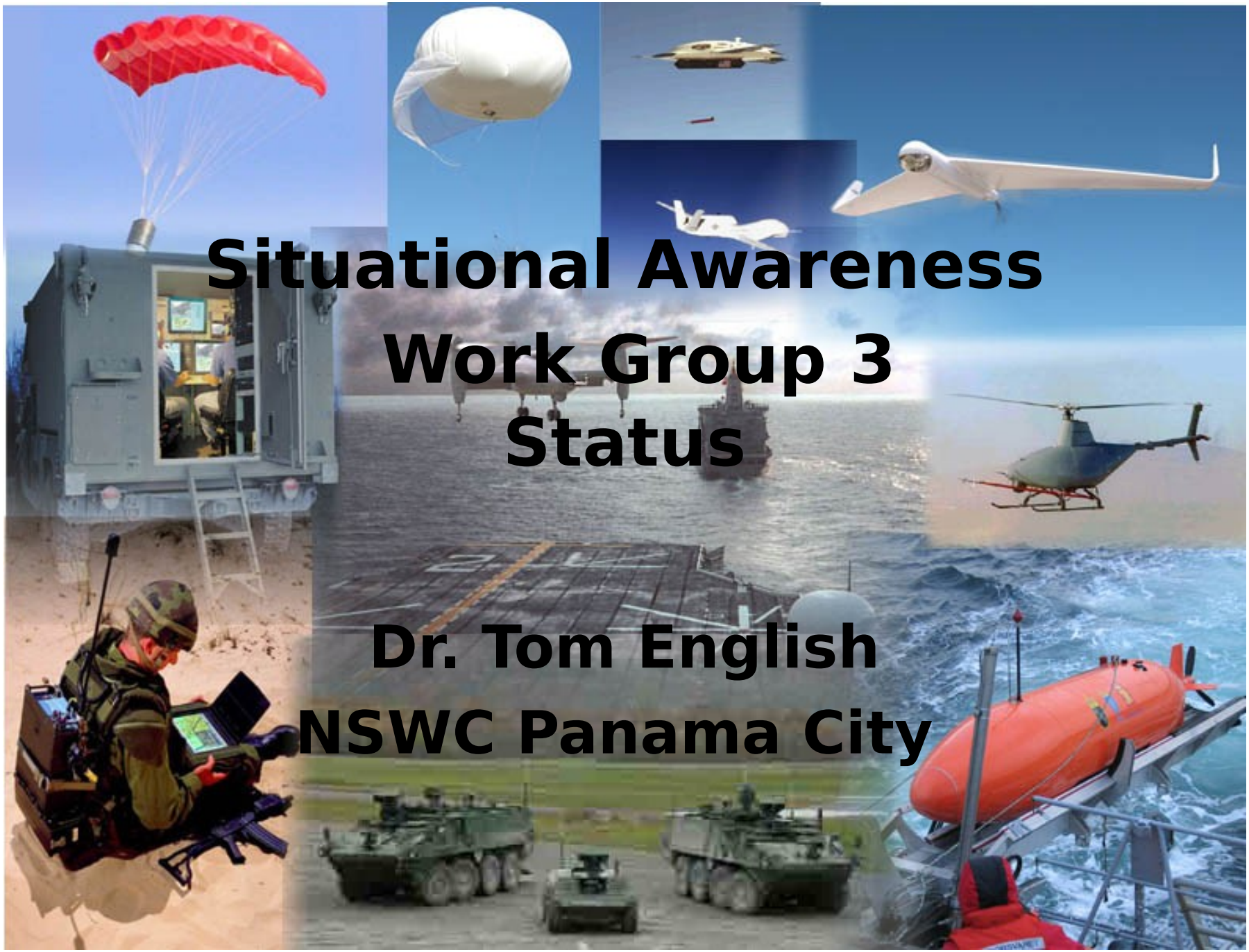
The unmanned systems shall provide safety design features to ensure safe recovery of all unmanned system equipment to include the platform and equipment.

Issue: Definition of UMS drives the scope of requirements.

Proposal: We recommend that scope be limited to systems that are designed to be returned or recoverable

Associated Guidelines

- All commands that initiate hazardous activities shall be self-terminating, and upon termination the UMS shall return to a known safe state.
- UMS shall provide weapon safety status to the authorized entity
- The UMS platform shall be capable of being returned to the original safe state or an equivalent level of safety.



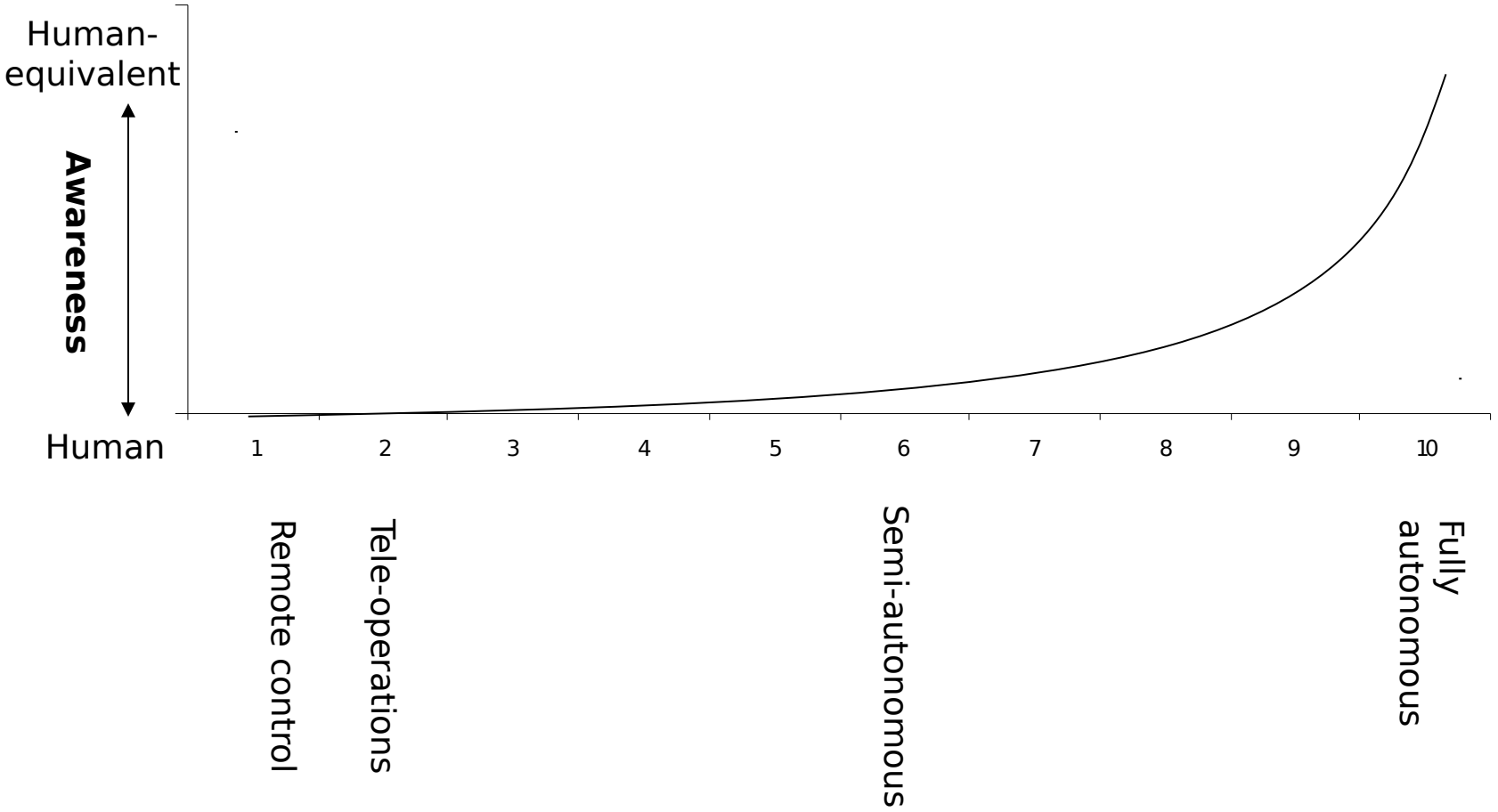
Situational Awareness
Work Group 3
Status

Dr. Tom English
NSWC Panama City

WG 3 Technical Products

- Revised DSP-4
- Developed supporting design safety guidance
- Created proposed UGV safety design guidance document
- Obtained proposed UUV safety design guidance document

Challenge - Addressing the Spectrum



Current DSP-4: The unmanned system shall be designed to provide control and situational awareness adequate to support safe operations.

Revised DSP-4: The unmanned system shall be designed to provide information, intelligence, and method of control (I^2C) to support safe operations.

WG 3 Issues Products

- Situational awareness and precepts
- Spectrum of autonomy linked to situational awareness
- A framework for standardizing UMS human performance
- A framework for UMS situational awareness

- **Issue: No standard framework to analyze UMS unique human performance factors**
  - Human-robot interaction ratio
  - Ability to interact with multiple vehicle/types of systems
  - Number of missions that can be supervised/monitored
  - Various environmental stimuli

Related Precepts:

OSP-2: The unmanned system shall not execute any operation without **commensurate situational awareness**.

DSP-2: The **unmanned system shall** be designed to **only respond to fulfill valid commands** from the authorized entity(s)

DSP-6: The **unmanned system shall** be designed to **prevent release/firing of weapons into unmanned system structure or other weapons**.

DSP-19: The unmanned system shall provide safety design measures **to identify the weapon being released/fired**

- **Issue: Machine Situational Awareness has never been characterized**
  - Formal characterization of machine situational awareness
  - Establishment of Machine SA evaluation criteria
  - Establishment of Machine SA evaluation techniques
  - Characterization of Machine SA effect on System Safety

Related Precepts:

DSP-4: The **unmanned system shall provide control and situational awareness** feedback adequate to support safe operations.

DSP-15: **The unmanned system shall** be designed to **minimize exposure of personnel, ordnance, and equipment to hazards generated/created by the unmanned system equipment**.

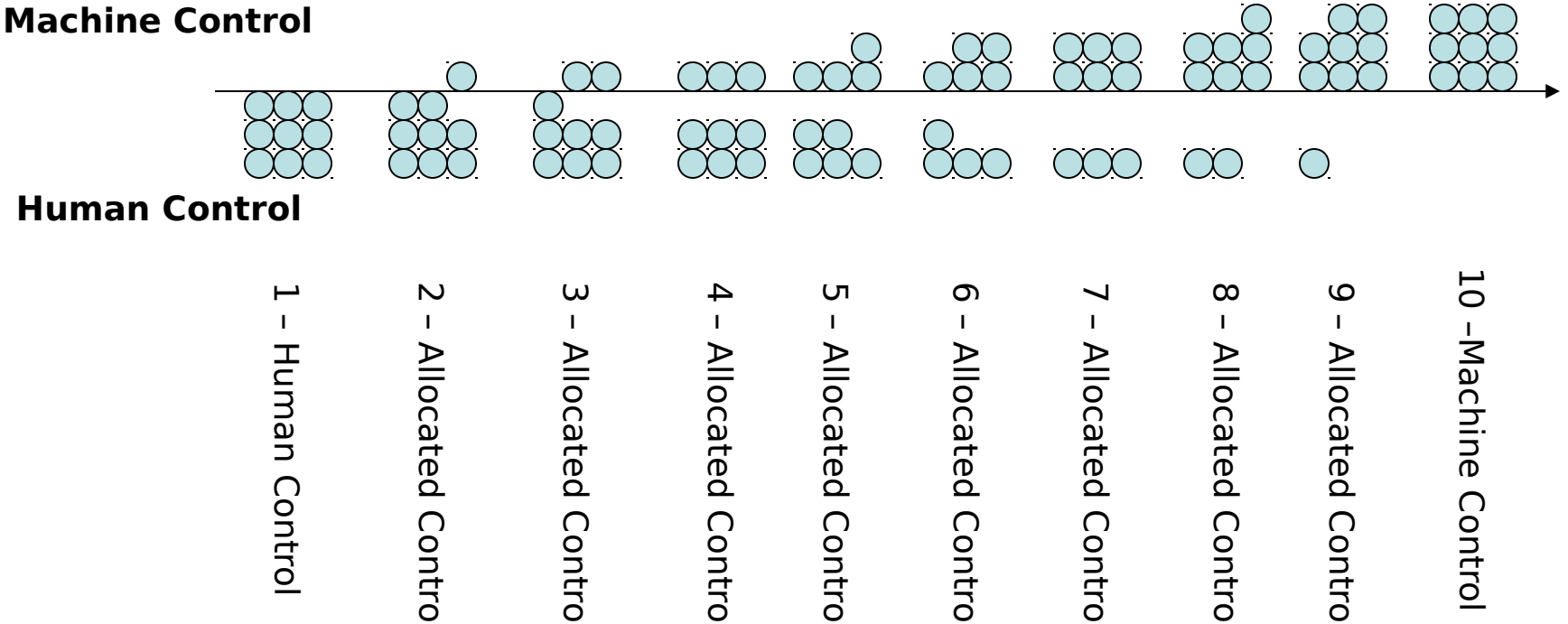
DSP-10: **The unmanned system shall safely change states and modes**.

Spectrum of Autonomy Linked to SA

Denotes individual safety-critical actions for which adequate SA must be defined.
i.e. arm the machine gun, steer to avoid obstructions, discriminate target, …

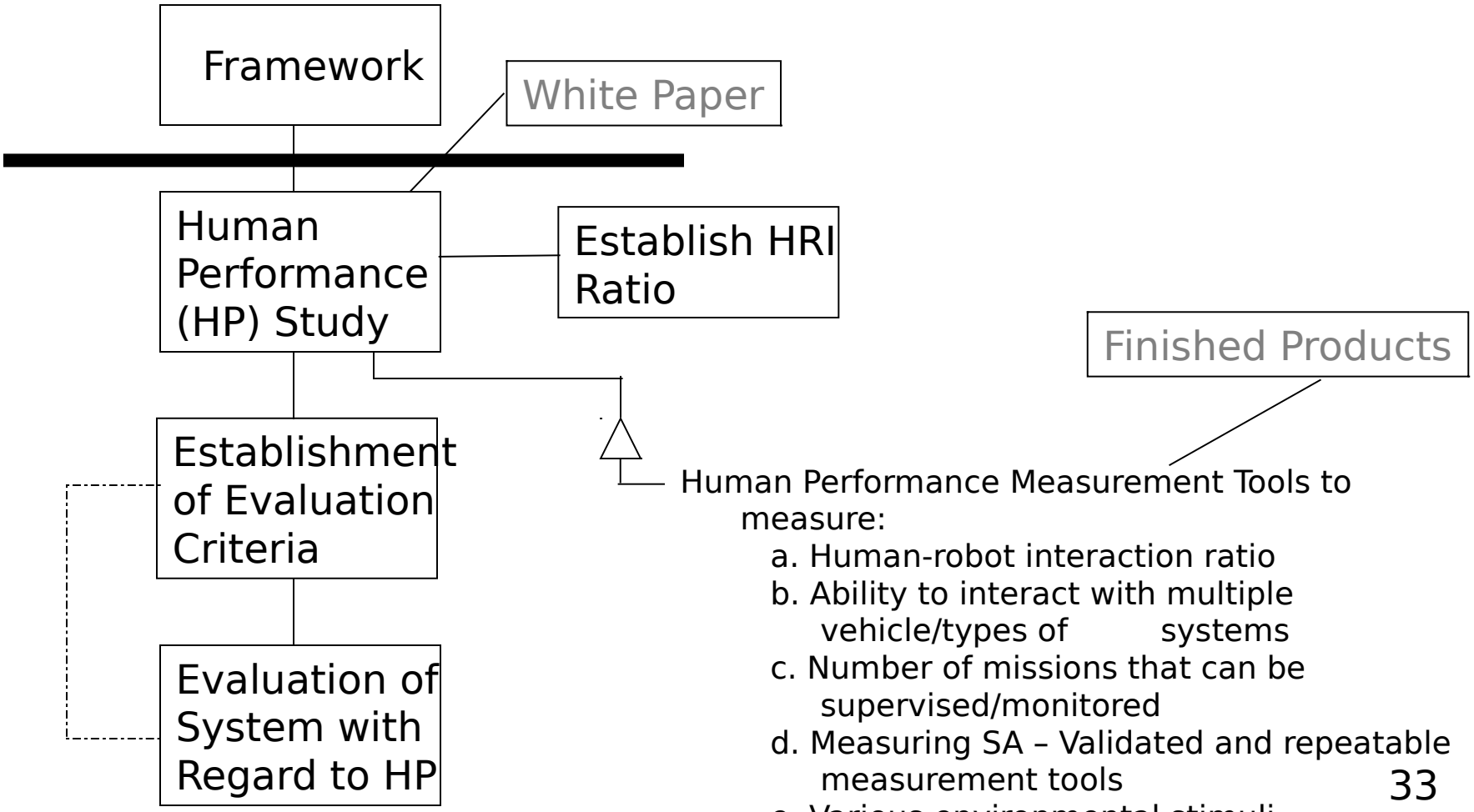
Position shows whether machine or human must have this SA.

Human SA requires Performance Measurement Criteria to evaluate.
Machine SA requires an original characterization since it is not currently defined.



A Framework for Standardizing UMS Human Performance

Where we are today


Framework
White Paper
Human Performance (HP) Study
Establish HRI Ratio
Finished Products
Establishment of Evaluation Criteria
Evaluation of System with Regard to HP
Human Performance Measurement Tools to measure:
a. Human-robot interaction ratio
b. Ability to interact with multiple vehicle/types of systems
c. Number of missions that can be supervised/monitored
d. Measuring SA – Validated and repeatable measurement tools
e. Various environmental stimuli

A Framework for UMS SA

Today, SA measurement criteria are insufficient for evaluating human & UMS interactions

Develop a Framework

White Paper

Characterize UMS Machine SA

UMS SA Performance Study

Establishment of Evaluation Criteria

Evaluation of System with Regard to UMS SA

Finished Products

Validated and repeatable tools to evaluate:

a. UMS SA across UMS systems types
b. UMS SA across various levels of automation
c. UMS SA effect on human interaction
d. UMS SA effect on system safety

Backup

Definitions:

- Information: Knowledge or data necessary for the safe operation of a UMS; obtained from the process of recognizing and interpreting data in the environment, memory and recall of facts, and/or communication.
- Intelligence: The capacity of a UMS to acquire, comprehend, and apply information.
- Method of control: The means or manner in which an operator interacts, influences, or directs an unmanned system; a function of three non-exclusive system attributes:
  - Mode of control
  - Level of authority
  - Level of control

Definitions (cont):

- Mode of control: The means by which a UMS receives instructions governing its actions and feeds back information.
  - Remote control
  - Teleoperation
  - Semi-autonomous
  - Fully autonomous

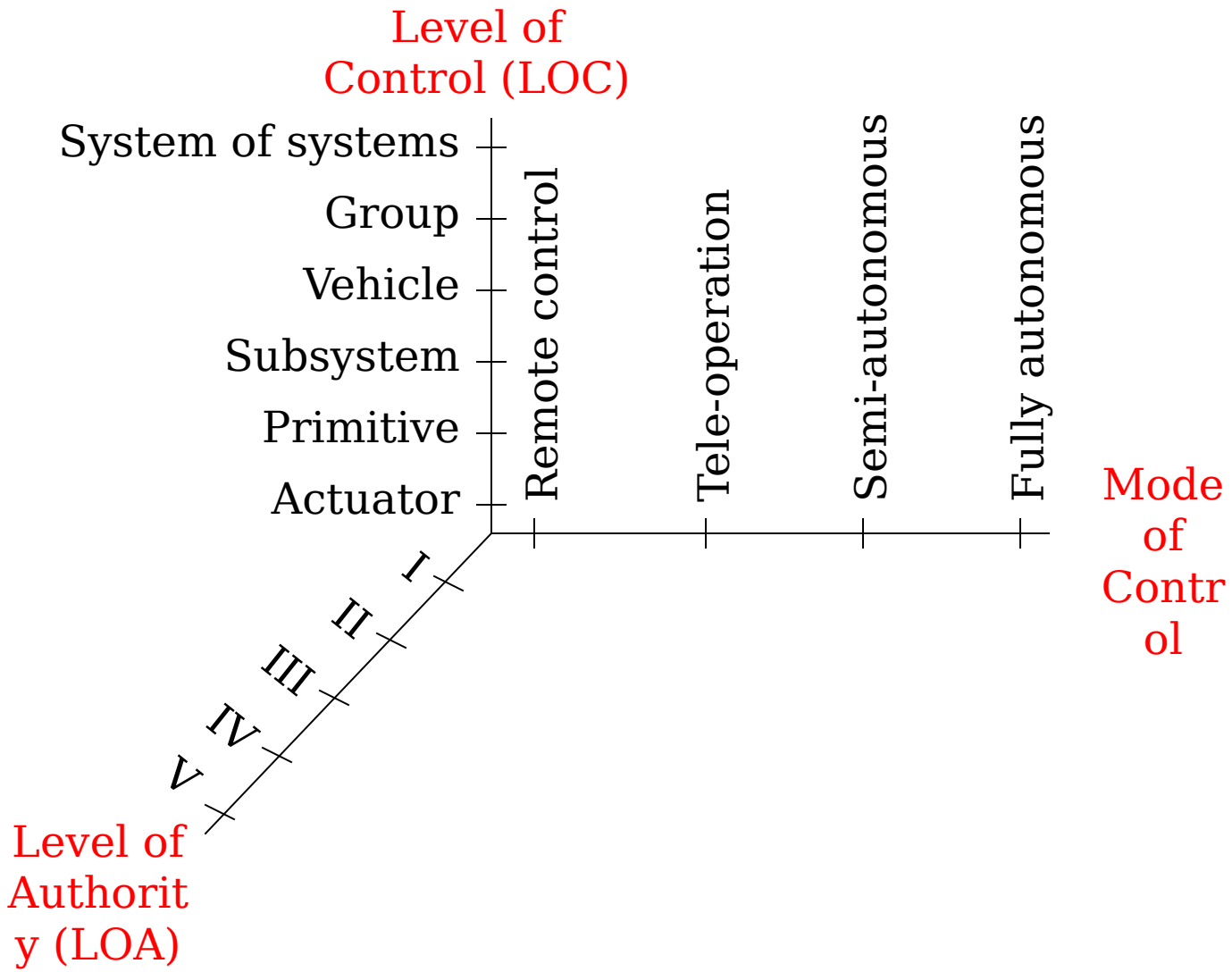
Definitions (cont):

- Level of authority: The degree to which an entity is invested with the power to access the control and functions of a UMS.
  - Level I – Reception and transmission of secondary imagery or data
  - Level II - Reception of imagery or data directly from the UMS
  - Level III - Control of the UMS payload
  - Level IV - Full control of the UMS excluding deployment and recovery
  - Level V – Full control of the UMS including deployment and recovery

Definitions (cont):

- Level of control: Locus at which a controlling entity interacts, influences, or directs a UMS(s).
  - Actuator
  - Primitive
  - Subsystem
  - Vehicle
  - Group of vehicles
  - System of systems

Method of Control



Command and Control Work Group 5 Status

Steve Mattern
Apogen Technologies

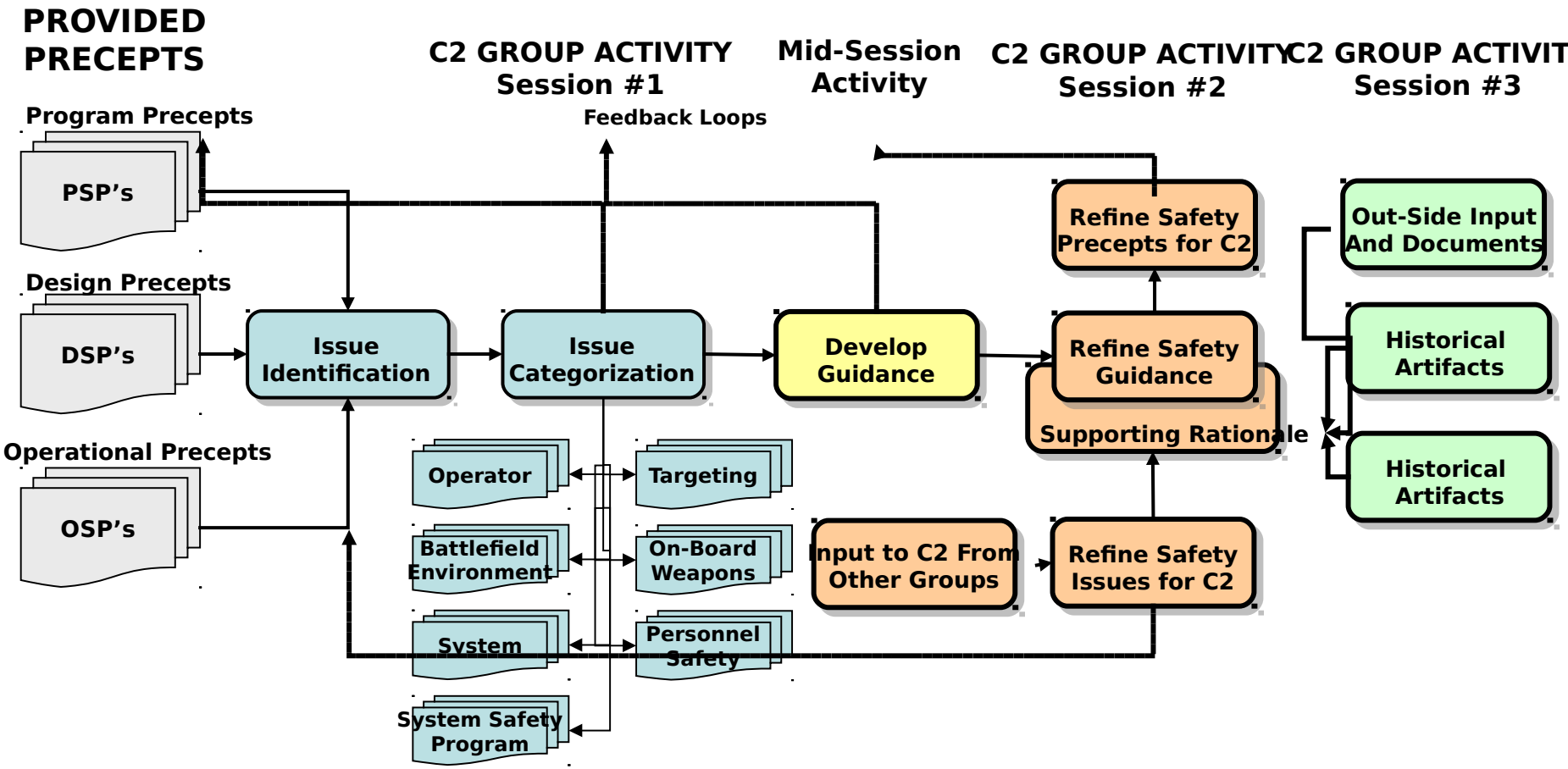
WG Membership

- Work Group Members
  - Steve Mattern (Apogen Technologies) Moderator
  - Billy Arnold (General Dynamics)
  - Ed Spratt (Navy)
  - John Canning (Navy)
  - Michael Dunn (Army)
  - Eugene Gonzales (Navy)
  - Martha Meek (Army)
  - Helmut Portmann (Navy)
  - Ron Price (Army)
  - Mike Zemore (Navy)
  - Rachael Fabyanic (Navy)
  - Frank Albert (Navy)
  - Steve Castelin (Navy)

COMMAND AND CONTROL WORK GROUP #5

- **Focused on the Command and Control Issues Involved with Unmanned System**
- **The Command and Control Issues Tended to be Functionally Linked With Other Work Groups…So the Issues Became Nearly All Inclusive (e.g., Weapons, Modes & States, Situational Awareness, etc.)**
- **Three Work Group Sessions…with Reviews/Discussions Between Sessions**
- **Started with Safety "Issues"…and, Worked Toward Program or Design Safety Guidance**
- **Precepts Mapped to Safety Issues**
- **Concluded with "Rationale" to Support Program and Design Safety Guidance**

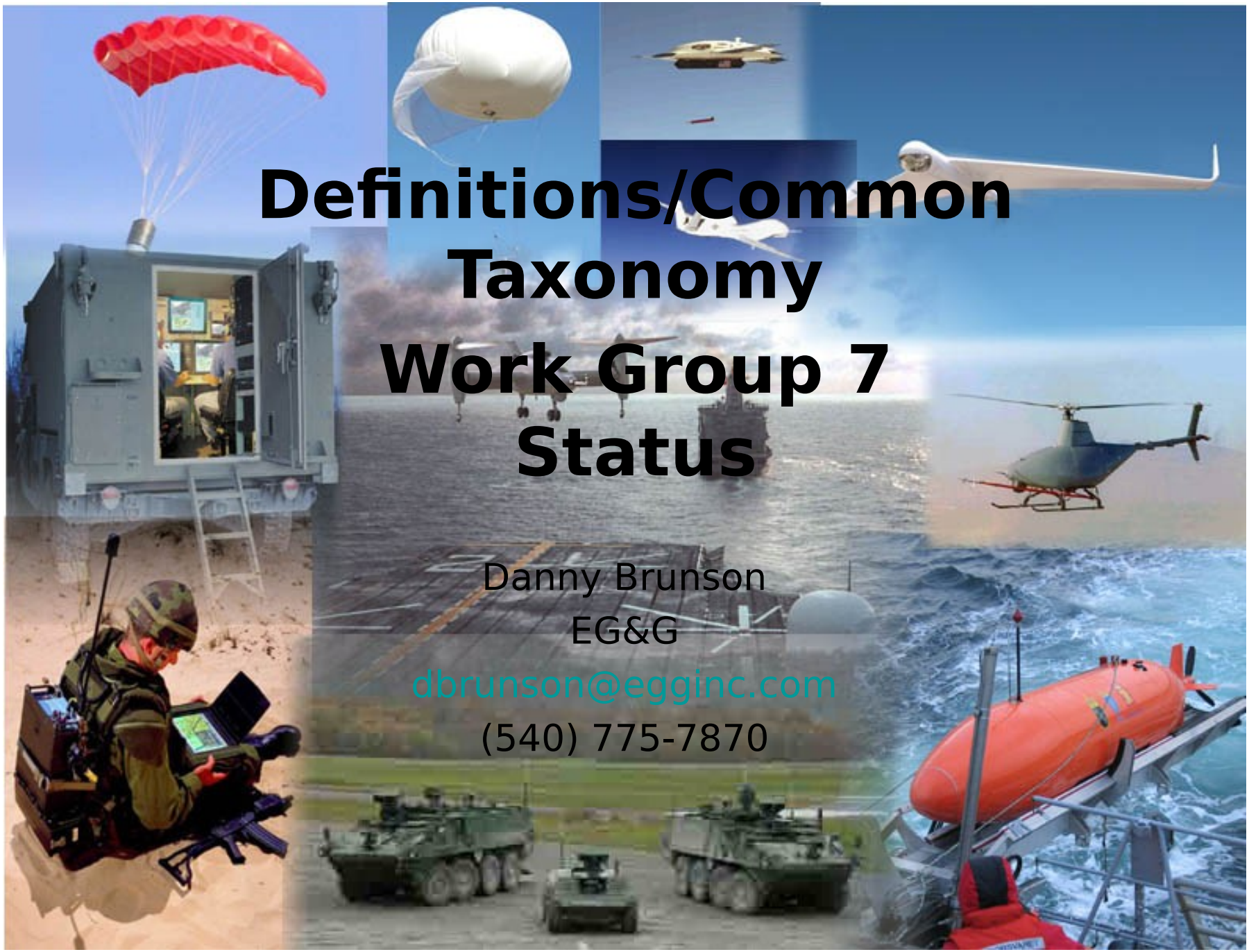
COMMAND AND CONTROL WORKING GROUP



UNMANNED SYSTEMS
DRAFT PROGRAM AND DESIGN SAFETY GUIDANCE

ISSUE	PRECEPT NO. Rev B	PRECEPT	PROGRAM AND DESIGN GUIDANCE	GUIDANCE RATIONALE
		by the communication.		
3.10.2 Operations			• The system should be designed to minimize the safety risk to the general public, system operators and maintenance and support personnel. • The system should be designed to minimize the risk of environmental contamination, pollution, or destruction	• The system should be designed to meet or exceed NEPA, OSHA, PESHE, etc. requirements for the protection of personnel, the system asset and the environment.
3.10.3 Operational Recovery	DSP-29	• The unmanned systems shall provide safety design features to ensure safe recovery of all unmanned system equipment to include the platform and equipment.	• The system should be designed to include a concept for safe recovery and re-initialization of system to a defined and known safe state when command and control authority is temporarily (either intermittent or long-term) lost in an operational or test environment	• It is essential for the operator to know the system mode or state upon system recovery. • This is to ensure the operator(s) are still controlling the same asset. This is a method of preventing cross control to verify that the C2 system is controlling the correct entity • There must be a level of assurance that a recovered asset is safe in terms of system mode or state
3.10.4 Emergency Contingency and/or Recovery	DSP-12 DSP-23	• The unmanned system shall be designed to provide means to identify state and/or mode of the system to the authorized entity(s). • The unmanned system shall be designed to support options for operational or emergency contingencies.	• Emergency [illegible] procedures should be considered for emergency recovery of the UMS by operators or first responders	• This is a continuation of 3.10.3 but for the specific case of emergency recovery by either operators or first responders • It is essential that procedures are developed for first responders to safe a UMS or a UMS weapon system
3.11 Certification of Intended (Qualified) Operator	OSP-6	• Only authorized, qualified and trained personnel, with the competencies, skills and experience, using approved procedures will operate or maintain the unmanned system	• Guidance provided in 1.2	• If the system has no capability to detect an authorized user, it is important to preclude the ability of a hostile or enemy to turn the machine against friendly forces • We do not want loss of asset or personnel due to incorrect use or maintenance
3.12 Man/Machine Interface	DSP-2	• The unmanned system shall be designed to only respond to fulfill valid commands from the authorized entity	• The system shall be designed to respond to fulfill authorized operator commands • The system should be designed to challenge commands/input that exceed system capabilities or command set parameters	• The HMI should receive the necessary design attention and robustness when operators are controlling safety-critical system • Illegal commands should not default to legal command
3.13 States and Mode Management	DSP-8	• The unmanned system shall be designed to prevent hazardous system	• Unmanned vehicle design shall include capabilities for end game scenarios as appropriate for the	• The initialization of a system into a specific state or mode, or the transition of states and

EXAMPLE PAGE



Definitions/Common Taxonomy Work Group 7 Status

Danny Brunson
EG&G
dbrunson@egginc.com
(540) 775-7870

WG Membership

- Work Group Members
  - Danny Brunson (EG&G), Moderator
  - Scottie Allred (MARCORSYSCOM)
  - Mary Ellen Caro (NOSSA)
  - Brad Cobb (NSWCDD)
  - Bill Christian (SED/L^3)
  - Clif Ericson (EG&G)
  - Randy Mann (SED/L^3)
  - Steve Mattern (Apogen Technologies)

Progress

- Identified Pertinent References
- Compiled Relevant Definitions
- Identified Needed Definitions
- Reviewed Definitions
  - Prioritized List
    - Cat 1 - 4
  - Selected most appropriate definitions
  - Prepared Draft Definitions

Pertinent References

- MIL-STD-882C
- MIL-STD-882D
- Joint Publication 1-02, DoD Definitions (http://www.dtic.mil/doctrine/jel/doddict/)
- ANSI/RIA R 15.06-1999
- STANAG 4586, Standard Interfaces of UAV Control System (UCS) for NATO UAV Interoperability
- INCOSE Systems Engineering Handbook
- JSSSH, Joint Software System Safety Handbook
- Joint Robotic Program Master Plan FY2005
- Army Regulation 385-16, System Safety Engineering and Management
- FAA System Safety Handbook
- USAF System Safety Handbook, 2000
- SAE ARP 4761, Aerospace Recommended Practice, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment
- SAE ARP 4754, Aerospace Recommended Practice, Certification Considerations for Highly-Integrated or Complex Aircraft Systems
- MIL-HDB-764
- AAP-6 (V) modified version 2, NATO Terms and Definitions
- MIL-STD-1316E, Fuzes
- MIL-STD-1910A
- MIL-STD-1901A
- IEEE 1228
- EIA SEB-6A
- DOE M 4401
- NASA-GB-8719.13
- AOP 38
- DAU Glossary 11th Edition
- Defense Acquisition Guidebook
- MILSTD 2105
- MILSTD 464
- MILSTD 882E (draft)
- NIST Special Publication 1011

Example

Term	Source	Definition	Cat	Comments
Design Safety Precept (DSP)	P	General design guidance intended to facilitate safety of the system and minimize hazards. Safety Design Precepts are worded to influence but not dictate specific design solutions.	1	

Plans

- Ground Rules
  - If there is an official definition for a term from a recognized source we will use that definition without modification.
  - If multiple recognized sources have different definitions we will select the most appropriate.
  - If there is not an official definition from a recognized source we will propose a definition for adjudication.
  - If an official definition is not satisfactory we will provide an additional alternate definition for adjudication.

Plans

- Complete Workgroup Review
- Establish baseline definitions
  - Category 1 and 2
- Provide recommended baseline for ISSC
- Begin process of resolving differences with other organizations after ISSC

Summary

- **Held three workshops**
- **Government/industry/academia teams developed draft safety precepts, rationale & design guidance**
  - **All Services and numerous program reps participating**
- **Preparing for ISSC panel discussion on 2 August 2006, Albuquerque**
  - **Next events:**
    - **AUVSI (29 – 31 Aug 2006)**
    - **NDIA Systems Engineering (23 – 26 Oct 2006)**
- **Will continue to refine precepts and safety design guidance after each event in preparation for publication**